PRESIDIO™

QUOTE: [redacted]
DATE: 07/23/2023
PAGE: 1 of 1

TO:
Williamson County
Thomas Gillespie
301 SE Inner Loop Suite 106
Georgetown, TX 78626

thomas.gillespie@wilco.org
(p) 512-943-1108
(f) (512) 943-1672

FROM:
Presidio Networked Solutions Group, LLC
Daniel Guzman
10415 Morado Circle
The Campus Building 1
Suite 320
Austin, TX 78759

dguzman@presidio.com
(p) +1.512.795.7146

Customer#: [redacted]

Contract Vehicle: Texas DIR-CPO-4859 Cybersecurity Products and Services

Account Manager: Daniel Guzman
Inside Sales Rep: Greg Hubbard
Title: Security - Application Security Audit

#	Part #	Description	Unit Price	Qty	Ext Price
1	PS-SVC-CYB-FF	Fixed Fee Cyber Security Services **Deliverable:** Project Initiation	$0.00	1 0000	$0.00
2	PS-SVC-CYB-FF	Fixed Fee Cyber Security Services **Deliverable:** Vulnerability scanning comple ion	$20,448.00	1 0000	$20,448.00
3	PS-SVC-CYB-FF	Fixed Fee Cyber Security Services **Deliverable:** Project Closure	$13,632.00	1 0000	$13,632.00

Sub Total:	**$34,080.00**
Grand Total:	**$34,080.00**

This quote is governed by Terms and Conditions of Texas DIR-CPO-4859 Contract.
State of Texas Vendor D 17605152499
Standard-Terms-for-Purchase-of-Services or Goods
Quote valid for 30 days from date shown above.
Prices may NOT include all applicable taxes and shipping charges
All prices subject to change without notice. Supply subject to availability.

Purchase Order should be issued to:
Presidio Networked Solutions Group, LLC
7701 Las Colinas Ridge #600
Irving, TX 75063

Pursuant to this contract your PO must reflect the following contract:
Texas D R-CPO-4859
Tax ID# 76-0515249; Size Business: Large; CAGE Code: 639L4; DUNS#11-436-9671; CEC 15-506005G
Credit: Net 30 days (all credit terms subject to prior Presidio credit department approval)
Delivery: FOB Destination

No signed quote. PO required.

PRESIDIO®

Application Security and Infrastructure Assessment

STATEMENT OF WORK

WILLIAMSON COUNTY

27-Jul-2023

www.presidio.com

PROPOSAL TEAM

Name	Company/Function	Email
Daniel Guzman	Presidio Account Manager	dguzman@presidio.com
David Rubel	Presidio Solution Architect	drubel@presidio.com

CHANGE REVISION RECORD

Revision	Date	Author	Notes
V0.1	17-Jul-2023	David Rubel	First Client Release
V1.0	19-Jul-2023	Ted Kilgore	RAP Review & Approval
V1.1	27-Jul-2023	Adam Barber	Adjust milestones
V2.0	27-Jul-2023	Ted Kilgore	RAP Review & Approval

1 EXECUTIVE SUMMARY

1.1 Background

Williamson County ("Client") has a recent initiative to validate the security posture of two of its business critical applications and their supporting infrastructure.

The goal of this assessment is to provide an understanding of the business and technical risks the organization is currently incurring. In order to attain this visibility, Williamson County is requesting that Presidio perform an assessment of these applications and the compute infrastructure that runs them, to provide a clear picture of the current risk levels and suggested remediation tasks.

1.2 Scope of Services

1.2.1 Engagement Management and Control

- **Engagement Management level**
  - Standard
    - Status meeting frequency – Weekly
    - Engagement Kickoff
    - Deliverable Presentation

1.2.2 Web Application Assessment

- Authenticated scanning
  - 2 production environment application(s):
    - Laserfiche
    - DEMS (Digital Evidence Mgt System)
  - Up to 2 role(s) per application

1.2.3 Internal Vulnerability Assessment

- Up to 20 Hosts
  - including web servers, application servers, database servers, file servers, other servers supporting these applications.
- Network scanning location(s): 1
- Testing to be performed during business hours

2 METHODOLOGY AND APPROACH

2.1 Engagement Management and Control

Detailed project planning is key to ensuring that the proposed engagement will meet requirements and help to reduce the risk of an ineffective project.

2.1.1 Standard

- Identify and schedule Presidio resources
  - Identify and schedule Presidio resources as appropriate to the engagement
- Hold kickoff meeting with key stakeholders
  - Review details of scope of work and methodology
  - Introduce key project team members and define roles and responsibilities
  - Review timelines, meetings, and additional requirements
  - Schedule implementation for discovery software
  - Schedule status meeting and other recurring touchpoints, as required
- Conduct status meetings at a frequency defined in this document
  - Review engagement progress
  - Identify engagement risks
  - Identify upcoming tasks
  - Request any additional customer or Presidio involvement
- Maintain and distribute engagement status report and schedule
  - All documents provided in Presidio formats
- Schedule Deliverable Presentation
  - Schedule mutually agreeable deliverable presentation

2.2 Web Application Assessment

Web Applications continue to present serious exposures to many customers. Presidio's Web Application testing extends the external or internal testing to include evaluation of the controls and function of web applications, and the associated vulnerabilities (including the OWASP Top 10. Examples include cross-site scripting, XML/SQL injection, input attacks, and similar).

The following tasks will be performed:

- Scoping
  - Validate URLs and testing windows with customer
  - Validate customer contact information
  - Collect any application documentation

- Validate any credentials and roles for in-scope authenticated testing

- Discovery and Application Scope
  - Review all application documentation
  - Perform application discovery
    - Manual walk-through of application and pages
    - Tool-based spidering
    - Brute-force content discovery
  - Map application and identify input/output fields
- Testing
  - Perform automated and manual testing, including:
    - Configuration and Deployment Management Testing
    - Identity Management
    - Authentication & Authorization Testing
    - Session Management (authenticated testing only)
    - Input Validation Testing
    - Error handling
    - Business Logic Testing (authenticated testing only)
    - Weak Cryptography Implementations
    - Client-side Testing
- Validation
  - Perform appropriate validation of any discovered issue
- Documentation
  - Prepare written document
    - Vulnerability
    - Any suggested remediation
    - Risk Score

2.3 Internal Vulnerability Assessment

Presidio will review the security of Client's network from inside the Internet perimeter. This will include both authenticated and unauthenticated scanning of in-scope hosts as defined in the scope of services. This will enable Presidio to provide a view of the risks based on privileged and service accounts, patching levels, as well as vulnerabilities with a high degree of confidence. Client will be able to clearly understand the risk should their perimeter protection be bypassed as is common in many current attack scenarios.

- Scheduling and target validation
  - Review target networks from scoping and discovery and validate
  - Determine scheduled testing windows
  - Validate customer and tester contact information
- Credentialed Network Scanning
  - Scan network with automated tools and customer-supplied administrative credentials
  - Determine vulnerabilities and patching status on all systems
- Active Directory Validation
  - Review existing accounts
    - Determine number and type of stale accounts
    - Review status of privileged accounts
  - Review password policy
- Vulnerability Validation
  - Review vulnerabilities and recommend priorities as appropriate
- Documentation
  - Prepare written report
    - Vulnerability
    - Risk Score
    - Suggested remediation
  - Prepare spreadsheet-based summary of vulnerabilities

3 DELIVERABLES

Deliverable	Description	Format
Status Report	Artifact which depicts key task areas, actions, owners, estimated completion dates, task status, and overall project status and delivered following each status meeting.	PDF
Executive Summary and Security Assessment Report	This report is made up of two sections. The first, an Executive Summary, will include summary of findings for all phases of the project and include a risk profile, high-level recommendations, and roadmap. The second section will be Detailed Findings. This section will show all findings from the project by phase with suggested remediations and references.	PDF
Vulnerability Registers	Sortable list of discovered vulnerabilities from external and internal vulnerability scanning activities.	Excel
Executive Presentation (optional)	At the customer's discretion, Presidio can conduct an executive presentation that will provide an overview of the assessment for all phases including approach, methodology, summary of findings, and summary of recommendations. The format will be appropriate for a non-technical, executive audience. A copy of the executive presentation will be provided.	PPT
Stakeholder Q&A (optional)	Prior to the optional executive presentation and at the customer's discretion, Presidio will hold a Q&A session with the project stakeholders to discuss the report and preview the Executive Presentation. This Q&A will occur after the customer's review of the document, and will not be a risk-by-risk review of the published report	None

Deliverables will be released via secure exchange only to the Client project sponsor or to others with written permission from the project sponsor.

Final presentations and closeout must be completed within thirty (30) days after the day the original documentation deliverable is released to Client. If the deliverable presentations are not completed in this timeframe, Presidio will consider this phase completed and will invoice accordingly.

4 ASSUMPTIONS

Presidio made the following assumptions when developing this Statement of Work. These assumptions serve as the foundation to which the project estimate, approach, and timeline were developed. Any changes to the following assumptions must be processed using the procedures the section titled “Project Change Request Process.”

4.1 General

The following project assumptions are made and will be verified as part of the engagement:

- All Presidio activities will take place during normal working hours (Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding holidays) unless noted as “Off Hours” in this SOW.
- Any items or tasks not explicitly listed as in-scope within this SOW are considered to be outside of the scope and not associated with this SOW and price.
- If integration of the product is performed at a Presidio facility, then transfer of ownership (acceptance) occurs upon the receipt and integration of goods at Presidio, regardless of shipment, as manufacturers will not accept returns of opened products.
- Changes to the Design, Equipment List, or proposed timeline presented to Client in this SOW will require a Project Change Request. A Project Change Request could impact the cost of the project
- Presidio will not be held responsible for troubleshooting networks, applications and/or hardware if Client has no formal change management documented processes and policies
- Presidio may engage subcontractors and third parties in performing a portion of this work.
- Some activities included in this project may be performed on Presidio’s premises.
- Additional required tasks discovered after the execution of this SOW that are not mentioned in this SOW will require a Project Change Request.
    - Presidio will provide clear guidance on the changes required to ensure optimal deployment.

4.2 General Client Responsibilities

The following items are listed as responsibilities of Client for this engagement. Client is responsible for performing the items and activities listed in this section or arranging for them to be performed by a third-party if appropriate.

- Provide a single Client point of contact with the authority and the responsibility of issue resolution and the identification, coordination, and scheduling of Client personnel to participate in the implementation of the SOW.
- Participate in any required design sessions or workshops.
- Supply current equipment configuration for review if applicable.

- Provide all required physical access to Client's facility (identification badge, escort, parking decal, etc.), as required by Client's policies; and provide all required functional access (passwords, IP address information, etc.), as required for Presidio to complete the tasks.
- Provide to Presidio all required IP addresses, passwords, system names, and aliases.
- Validate the site readiness prior to the dispatch of Presidio personnel to perform the services being contracted.
- Provide Presidio administrator access on appropriate devices for the completion of the engagement.
- Provide requested documentation or information needed for the project within two (2) business days, unless otherwise agreed to by all parties.
- Provide to Presidio all relevant Client information security and information technology policies and procedures.
- Provide to Presidio all requested information about and administrative access to Client's technical infrastructure for the duration of the project, including, but not limited to, each technology component described in each phase listed above.
    - For phases that include a Technical Configuration Review activity, remote access is required, AND administrative access must be sufficient to analyze the configurations of each technology component.
- Client will make all network and endpoint changes and configurations as required to integrate Presidio's tools.

4.3 Travel

Presidio has made the following assumptions for travel:

- Presidio assumes all work will be performed remotely

4.4 Internal Vulnerability Assessment

- Customer will provision a virtual host to Presidio's specifications or will provide connectivity and power for a Presidio-provided system. Customer will allow Presidio remote access to these systems to allow for internal scanning.
- Customer will provide VPN-based remote access to the provisioned virtual host or will allow other remote access as determined during the kickoff meeting
- The following specifications are required to run the necessary software during this phase
    - Windows Server 2012, 2016, 2019
    - (4) >= 2.4G vCPU
    - (16) GB RAM
    - (40) GB Hard Drive
    - Local admin rights

5 PRICING

Presidio is providing a Fixed Fee Price as part of this Statement of Work. Presidio will invoice Client based on the project milestone(s) listed below:

Milestone Name	Amount
Project Initiation	$ 0.00
Vulnerability scanning completion	$ 20,448.00
Project Closure	$ 13,632.00
Total	**$ 34,080.00**

Presidio will bill Client upon completion of each Milestone. Invoices may contain multiple Milestones.

If Client requires a change in the scope of work, the parties will negotiate in good faith to generate a written change order documenting the additional labor and requirements that will be mutually agreed upon by the parties prior to onset of the additional work.

If, in Presidio's reasonable discretion, completion of one or more of a project's milestones are subject to a material delay due to factors outside of Presidio's control, Presidio may invoice Client a prorated amount for work performed which reflects Presidio's current progress toward completing the milestone(s) at the time of any such delay.

Payment terms are subject to credit department approval and will be negotiated and documented on a valid purchase order or other financial document. If Client fails to provide a notice of acceptance or a statement of issues to be resolved within ten (10) business days of project conclusion, the project will be deemed accepted and Client will be invoiced.

5.1 Expenses

There are no anticipated travel or incidental expenses to be incurred by Presidio in association with the execution of this Statement of Work and therefore no expenses will be billed to Client.

5.2 Travel Time

Travel to and from the work site(s) by Presidio resources in association with the execution of this Statement of Work will not be charged to Client.

6 TERMS AND CONDITIONS

6.1 General

This service agreement is governed by DIR Contract Numbers DIR-CPO-4859 between Presidio and the Texas Department of Information Resources.

7 AUTHORIZATION TO PROCEED

The use of signatures on this Statement of Work is to ensure agreement on project objectives and the work to be performed by Presidio.

Presidio signature signifies our commitment to proceed with the project as described in this document. Please review this document thoroughly, as it will be the basis for all work performed by Presidio on this project.

This Statement of Work is valid for a period of sixty (60) days from the date that this Statement of Work is provided by Presidio to Client unless otherwise agreed to by both parties.

Williamson County

Bill Gravell Jr.
Bill Gravell Jr. (Aug 9, 2023 07:33 CDT)

Aug 9, 2023

Signature | Date

Bill Gravell Jr. | County Judge

Printed Name

Presidio

Edward Kilgore (Jul 27, 2023 14:57 CDT)

Jul 27, 2023

Signature | Date

Edward Kilgore | Director of Professional Services

Printed Name & Title

APPENDIX A – PROCESSES AND GUIDELINES

Presidio Process for Network Degradation or Outage

Presidio and Client will exchange specific contact information (including cell phone numbers) prior to starting any scanning or testing activities. Either party observing a service disruption will contact the other party. Presidio will stop running the scan tool and work with Client to determine why the disruption occurred and how to successfully complete the assessment without causing any further disruption. No denial-of-service (DoS) attacks will be intentionally initiated against any Client assets.

Process to Report Observed Incidents or Critical Risks

Presidio will contact the Client contact immediately if any critical risks are identified (those which present sufficient risk to warrant immediate remediation), including any observed incidents of attempted intrusion (from a party other than the authorized Presidio consultant[s]), while executing this engagement. Presidio will immediately provide to Client all information gathered relevant to the critical risk(s) identified.

Engagement Data Management

The deliverables produced from this engagement should be managed with strict policies and procedures due to the sensitive nature of the raw data collected during the engagement, and the associated findings Client's policies should specify which person(s) in an organization should have access to the data. Presidio consultants will store and transmit engagement-related data using appropriate encryption.